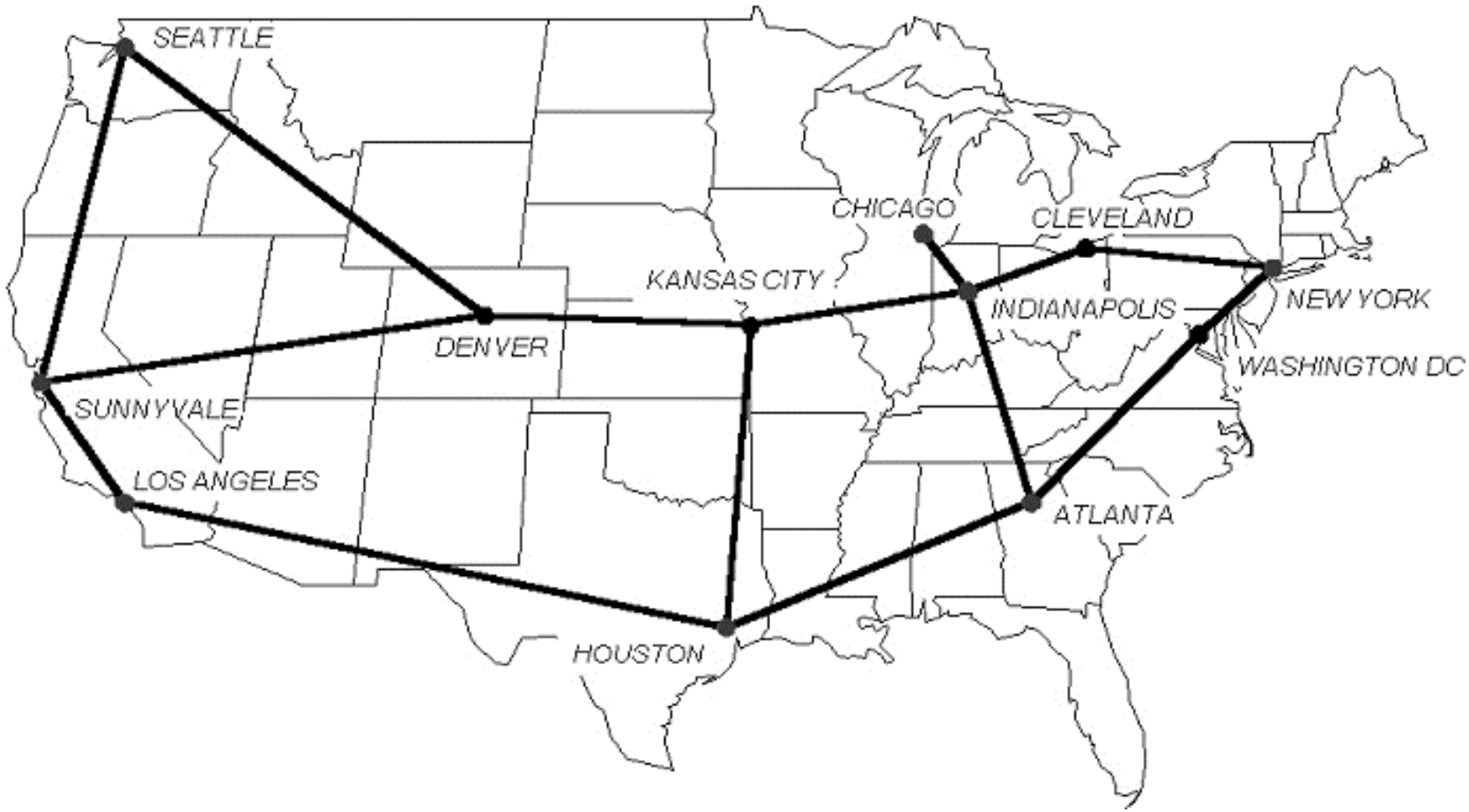
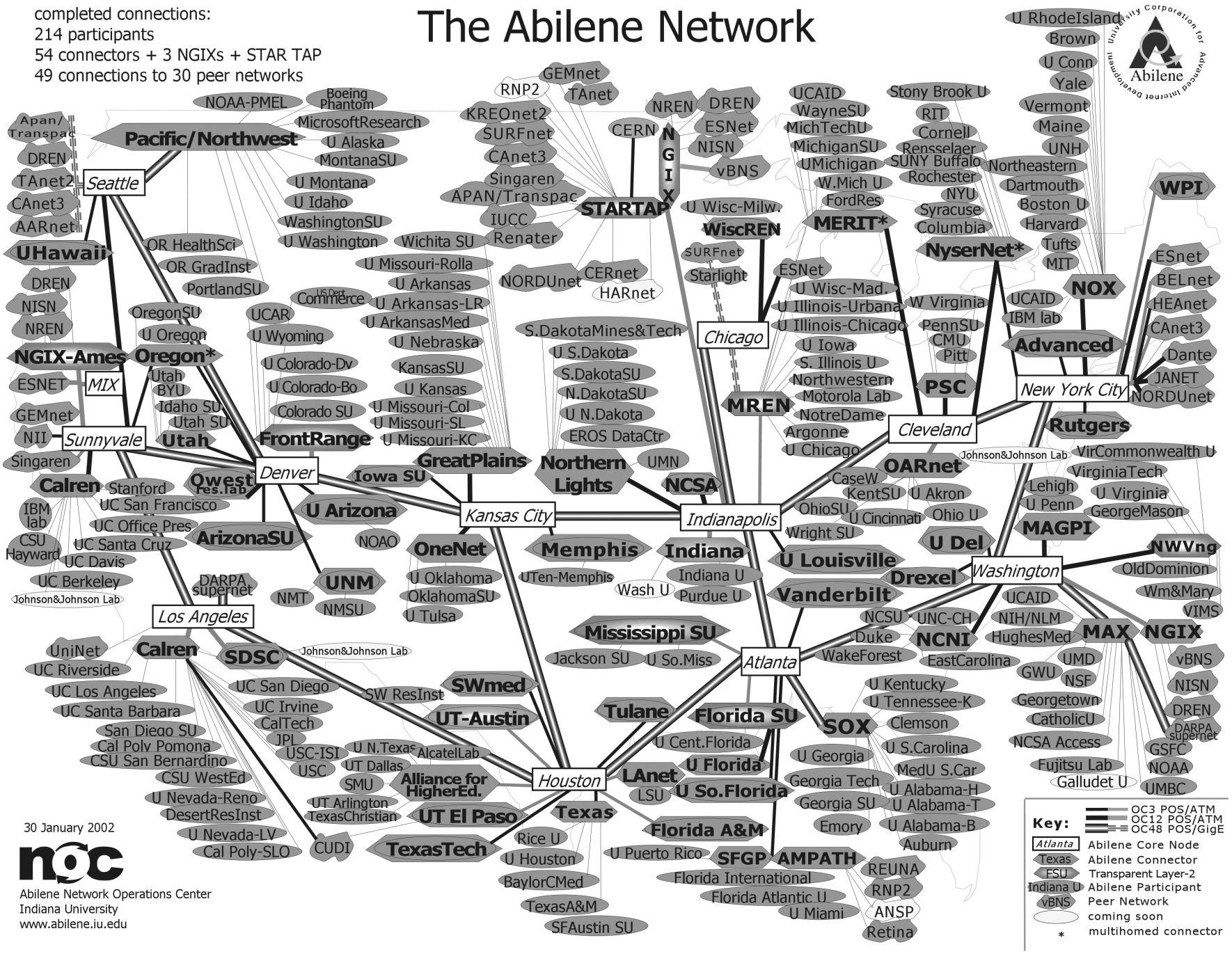
Abilene NetFlow Deployment

Mark Fullmer – OARnet / Ohio ITEC
maf@splintered.net

Abilene Network Backbone - February 2002




completed connections:
214 participants
54 connectors + 3 NGIXs + STAR TAP
49 connections to 30 peer networks
The Abilene Network
Abilene
University Corporation for Advanced Internet Development
Seattle
Sunnyvale
Los Angeles
Denver
Kansas City
Houston
Chicago
Indianapolis
Atlanta
Cleveland
New York City
Washington
Pacific/Northwest
STARTAP
NGIX
MERIT*
MREN
WiscREN
PSC
NyserNet*
Advanced
NOX
WPI
MAX
NGIX
MAGPI
OARnet
Rutgers
NCNI
SOX
Drexel
Vanderbilt
U Del
U Louisville
Indiana
Memphis
OneNet
GreatPlains
Northern Lights
NCSA
Iowa SU
Qwest
FrontRange
Utah
Oregon*
NGIX-Ames
Calren
ArizonaSU
U Arizona
UNM
SDSC
SWmed
UT-Austin
Tulane
Florida SU
LAnet
U So.Florida
Texas
Alliance for HigherEd.
UT El Paso
TexasTech
Florida A&M
SFGP
AMPATH
REUNA
RNP2
ANSP
Retina
Mississippi SU
Jackson SU
U So.Miss
Abilene Network Operations Center
Indiana University
www.abilene.iu.edu
30 January 2002
Key:
OC3 POS/ATM
OC12 POS/ATM
OC48 POS/GigE
Atlanta Abilene Core Node
Texas Abilene Connector
FSU Transparent Layer-2
Indiana U Abilene Participant
vBNS Peer Network
coming soon
* multihomed connector

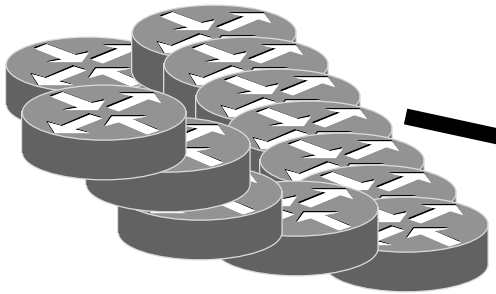
Deployment Motivations

- Traffic Engineering.
- Applications in use (port/protocol counts).
- DoS Detection.
- Monitoring deployment of emerging technologies (Multicast, QoS).
- Support of network traffic research efforts.

Architecture

- Four independent data analysis efforts.
- Routers (exporter) supports one data feed.
- Replicate the exports to multiple collectors.
- Post processed, anonymized data feed.
- Public web based access to select summarized reports.

Architecture



NetFlow exports (UDP)

Server running flow-fanout @ IU

12 Abilene core routers
Configured with sampled NetFlow (1/100 sampling)

Arbor

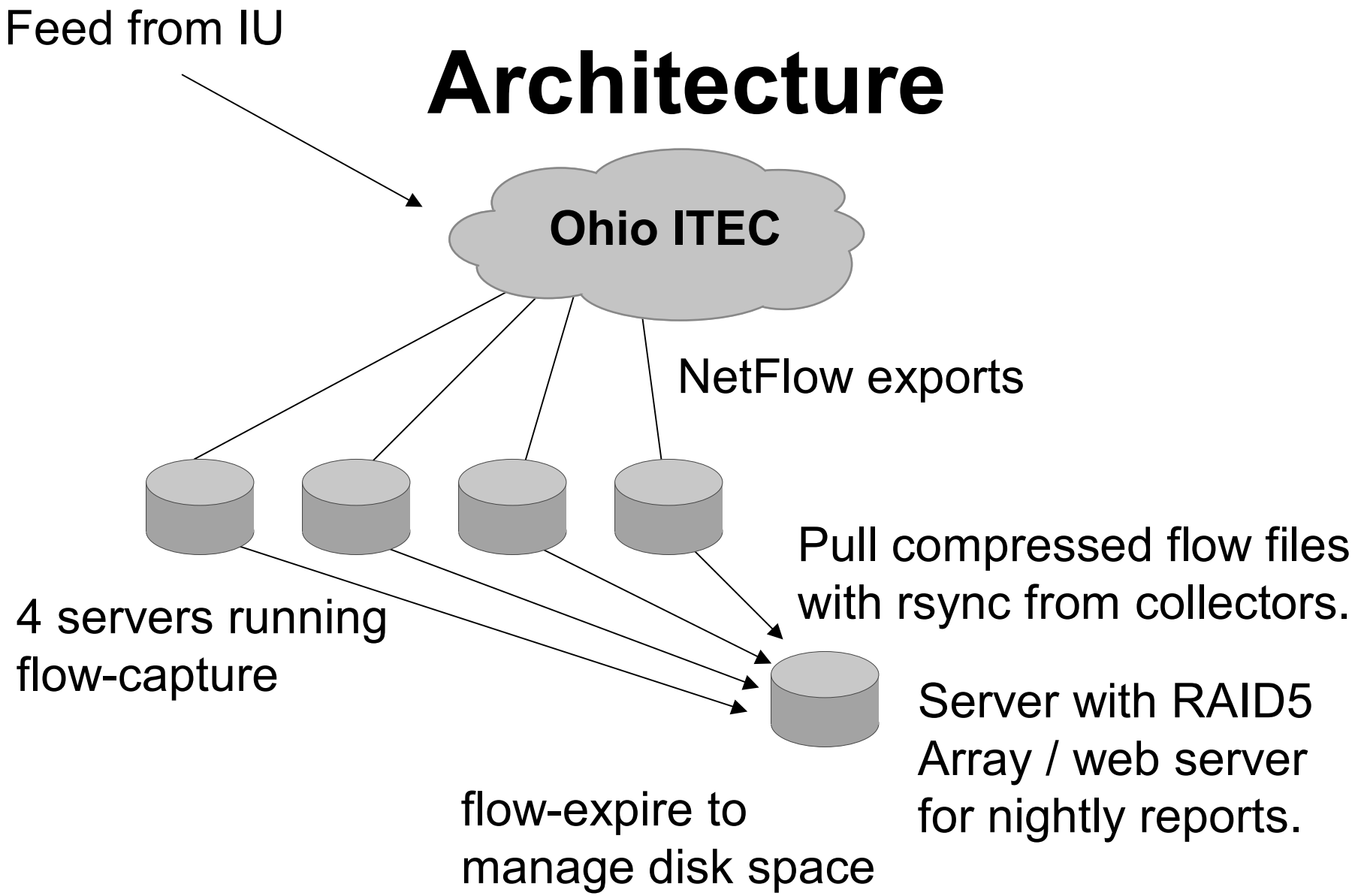
Asta

Ohio ITEC

Internet2.edu

Post Processed flows (ssh)

Architecture

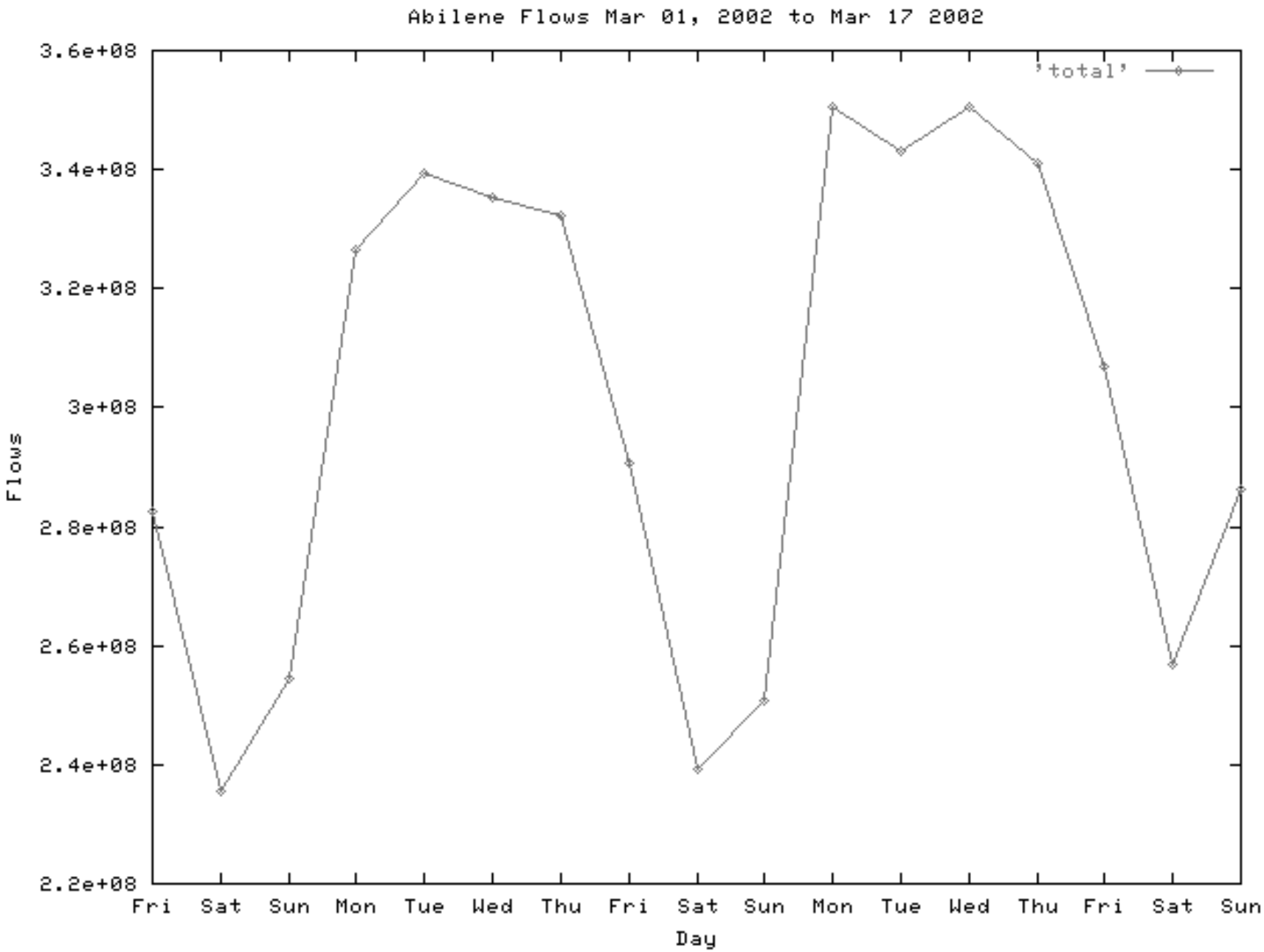


Architecture

- Fanout server supports multicast. Most implementation of NetFlow do not support multicast. Fanout data rate turned out to not be an issue.
- flow-fanout decodes and replicates exports. Decoding is required to instrument packet loss and data rates.

Architecture

- Collectors require SNMP access and BGP tables.
- SNMP is used to gather ifNames, and ifDescr. IfDescr has topology information encoded. Ie, what is an internal interface.
- BGP communities communicate policy used for some reports. Flows have tag field added.
- No need to duplicate this (type of) information in IPFIX…

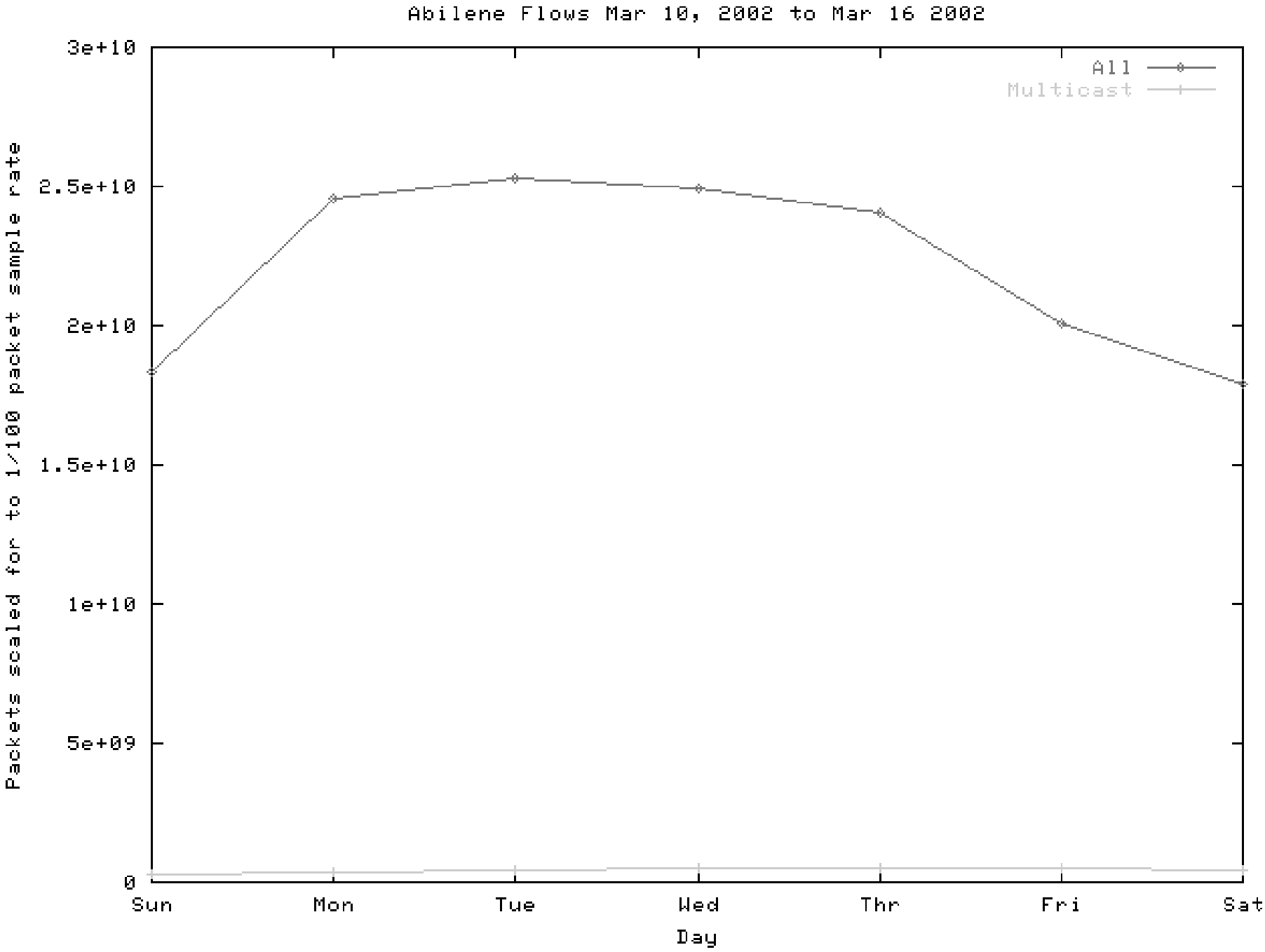

Abilene Flows Mar 01, 2002 to Mar 17 2002
'total'
Flows
3.6e+08
3.4e+08
3.2e+08
3e+08
2.8e+08
2.6e+08
2.4e+08
2.2e+08
Fri
Sat
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Sun
Day

Network wide daily report

# (percent totals)				
#				
# port	flows	octets	packets	duration
#				
nntp	1.874	15.596	7.204	4.203
FastTrack	16.226	7.545	10.854	11.194
Gnutella	9.685	4.822	9.205	15.187
commplex-link	0.006	2.794	1.167	0.009
Neomodus-Direct	0.285	1.569	0.873	0.972
ftp-data	0.589	1.301	1.675	1.024
5020	0.091	0.898	0.639	0.292
ssh	0.326	0.460	0.373	0.180
ftp	0.616	0.325	0.398	0.292
eDonkey-2000	0.506	0.316	0.393	0.582
0	0.054	0.315	0.147	0.061
http	3.959	0.312	1.652	0.833
Gnutella	0.803	0.238	0.481	0.615

Network wide daily report

# src AS	dst AS	flows	octets	packets
#				
UONET	0	0.124	1.673	0.923
CIT	NCSA-AS	0.001	1.214	0.553
SLAC	DFN-WIN-AS	0.082	1.197	0.582
SLAC	ITALY-AS	0.098	0.897	0.414
GEORGIA-TECH	FSU-AS	0.007	0.681	0.307
ITALY-AS	UPENN-CIS	0.021	0.607	0.255
CIT	ARGONNE-AS	0.001	0.600	0.321
BCNET-AS	MIT-GATEWAYS	0.034	0.558	0.283
UCLA	UTK	0.020	0.534	0.268
UCLA	NSFNETTEST14-AS	0.078	0.507	0.244
MIT-GATEWAYS	GEORGIA-TECH	0.013	0.476	0.245
GEORGIA-TECH	PENN-STATE	0.014	0.437	0.198
UONET	UW-MILWAUKEE-AS1	0.031	0.412	0.178
UONET	CONCERT	0.103	0.396	0.315
UONET	NSFNETTEST14-AS	0.043	0.391	0.184
COLORADOSTATEUNI	SLAC	0.005	0.356	0.147


Abilene Flows Mar 10, 2002 to Mar 16 2002
Packets scaled for to 1/100 packet sample rate
3e+10
2.5e+10
2e+10
1.5e+10
1e+10
5e+09
0
All
Multicast
Sun
Mon
Tue
Wed
Thr
Fri
Sat
Day

Collector Placement

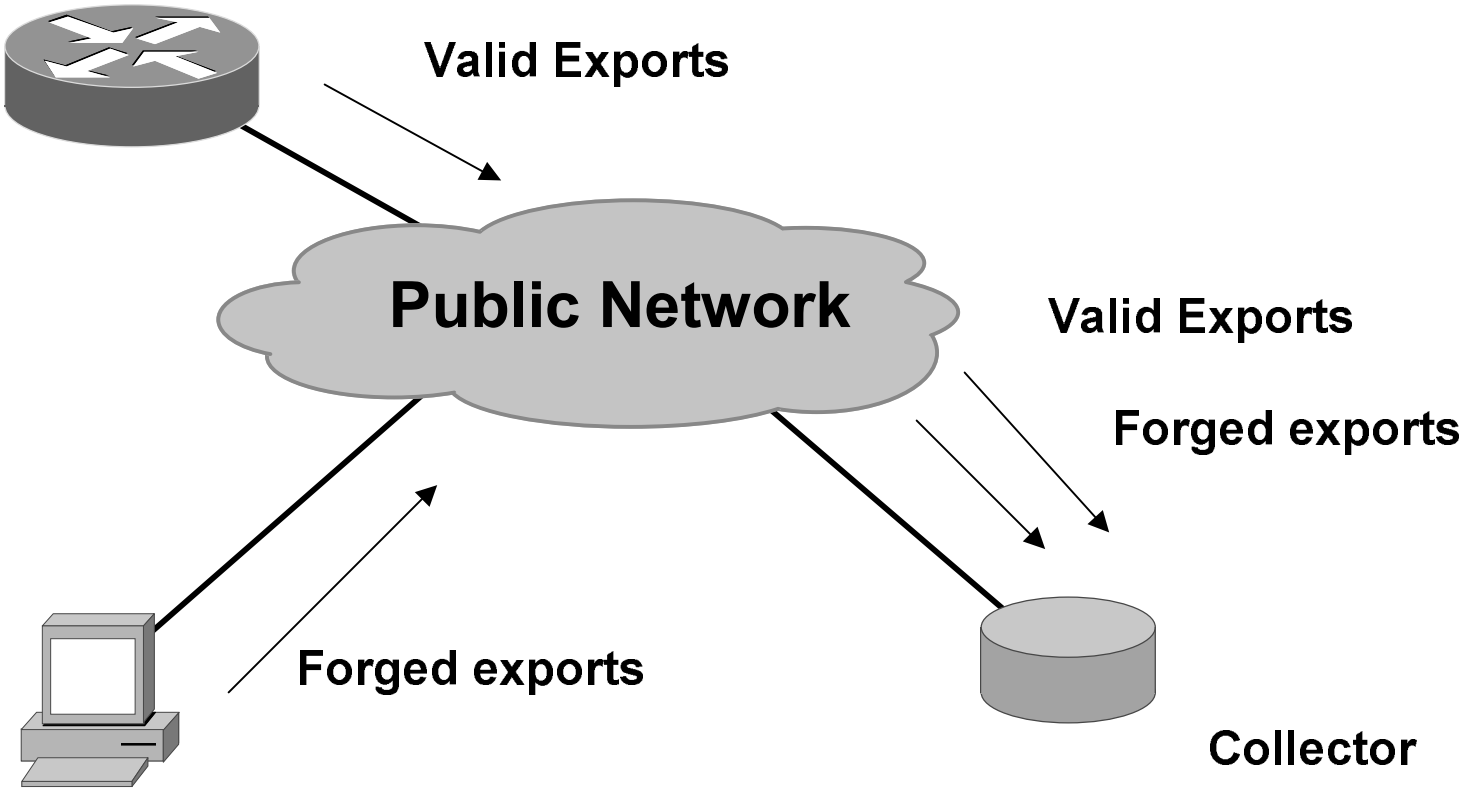
- Ideal place for collector is directly connected to the router or exporter.
- Not always practical or economical. Router now requires LAN interface.
- Colo facility issues (space, access, rack cost, etc).
- When collector is not directly connected DoS and spoofing issues arise.

Remote Collector Security

- Packet flood the collector.
- Send spoofed flows. NetFlow authentication is based on source IP. Some collectors can be configured to ignore it (user convenience).
- Spoofed flows can be detected by sequence numbers, but difficult to know it's an attack. Could be packet loss, router/linecard reload.
- Encrypted and/or authenticated tunnels can help but high CPU overhead.
- Middle ground – add authenticator to exports.

Remote Collector Spoofing

Router exporting flows.



Attacker knows router source IP and collector IP and port.
(not obvious to router operator that addressing information is only security)

References

- flow-tools: http://www.splintered.net/sw/flow-tools
- Abilene NetFlow page http://www.itec.oar.net/abilene-netflow
- Flow-tools mailing list: flow-tools@splintered.net
- Cisco NetFlow: http://www.cisco.com/warp/public/732/Tech/netflow/